REMARKS

In response to the Office Action mailed September 26, 2007, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks and have added new claims. The claims as now presented are believed to be in allowable condition.

Claims 1-49 were pending in this Application. By this Amendment, claims 50-51 have been added, and claim 9 has been amended. Accordingly, claims 1-51 are now pending in this Application. Claims 1,9, 10, 18, 26, 34, and 42 are independent claims.

Rejections under §102 and §103

Claims 1-49 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,832,210 (Akiyama et al.).

Applicants respectfully traverse each of these rejections and request reconsideration. The claims are in allowable condition because they patentably distinguish over the prior art.

Akiyama teaches a device and method for preventing a re-use of an identification code by an unauthorized user (Col. 2, lines 48-54). A transmission device 10 transmits signals to a receiving device 20 over communication path 30. The transmitted signals include transmitting identification information ID, control information X, a communication number k, and a certifier f_{KY}(ID, X, k). (Col. 11, lines 6-24). f is a unidirectional function, and KY is a certifying key (Col. 12, lines 21-28). Transmission device 10 transmits a signal several times to receiving device 20, each time incrementing the communication number k, and between distinct communications further incrementing k (Col. 11, line 46 through Col. 12, line 18). Receiving device 20, upon receiving a signal, confirms that the identification information ID is correct, that the communication number k is larger than any previously received communication number k, and then applies the

same certifying function f_{KY} using the same key KY and the received parameters ID, X, and k from the signal to verify the integrity and security of the signal. If the signal is verified, then operation X is carried out and receiving device 20 stores the received communication number k plus an addition number Δk. (Col. 12, line 35 through Col. 13, line 40).

Claims 1-8

Claim 1, as amended, recites a method of blocking attacks on a computer network. The method includes (a) receiving original packets and corresponding retransmit packets from a network, so each said original packet and corresponding retransmit packet belongs to a flow; and each said original packet and corresponding retransmit packet has a plurality of non-mutable field values, (b) hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet, (c) storing said validation signatures, (d) hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet, (e) comparing said validation signature to said test signature, and (f) if said test signature and said validation signature are not identical, terminating said flow.

The cited reference does not teach or suggest a method, which includes *hashing said non-mutable field values* of each said original packet to *produce a validation signature of each said original packet*, *hashing said non-mutable field values* of each said corresponding retransmit packet to *produce a test signature of each said corresponding retransmit packet*, *comparing said validation signature to said test signature*, and *if said test signature and said validation signature are not identical, terminating said flow*. Rather, Akiyama discloses applying a certifying function f_{KY} using key KY and the received parameters ID, X, and k from the signal to verify the integrity and security of the signal. If the signal

is verified, then operation X is carried out and receiving device 20 stores the received communication number k plus addition number Δk. However, Akiyama does not teach the aforementioned features.

Akiyama does teach applying a unidirectional function f_{KY} to parameters ID, X, and k (Col. 12, lines 21-34), and again applying the same function to received parameters ID, X, and k (Col. 13, lines 1-27). However, even if the application of unidirectional function f_{KY} is considered *hashing* (and Applicants do not admit that the application of unidirectional function f_{KY} is considered *hashing*), unidirectional function f_{KY} is applied to parameters ID, X, and k, and parameter k is not a *non-mutable field value*. Rather, communication number k is mutable because k changes with every transmission (Col. 11, line 62 through Col. 12, line 18; also see Figs. 9 and 10). Thus, Akiyama does not teach *hashing said non-mutable field values* of each said original packet nor does it teach *hashing said non-mutable field values* of each said corresponding retransmit packet.

In addition, even otherwise, Akiyama does not teach *hashing* said non-mutable field values of each said original packet to *produce a validation signature of each said original packet*, *hashing* said non-mutable field values of each said corresponding retransmit packet to *produce a test signature of each said corresponding retransmit packet*, and *comparing said validation signature to said test signature*. Akiyama does teach applying a unidirectional function f_{KY} to parameters ID, X, and k to form the transmitted signal Col. 12, lines 21-34), and again applying the same function to received parameters ID, X, and k to verify the signal (Col. 13, lines 1-27). However, the comparison of the claim is between *validation signature of said original packet* and *test signature of said corresponding retransmit packet*, while the comparison of Akiyama is between the received certifier S and the calculated certifier based on the other parameters also received together with S. Although Akiyama also teaches transmitting information several times consecutively, no comparison is made between certifiers (generated by unidirectional function f_{KY}) of different transmissions, but

rather between a received and a calculated certifier of the same transmission. Thus, Akiyama does not teach *hashing* said non-mutable field values of each said original packet to *produce a validation signature of each said original packet*, *hashing* said non-mutable field values of each said corresponding retransmit packet to *produce a test signature of each said corresponding retransmit packet*, and *comparing said validation signature to said test signature*.

Furthermore, Akiyama does not teach *if said test signature and said validation signature are not identical, terminating said flow*. Rather, Akiyama teaches performing control operation X and incrementing communication number k to ignore subsequent transmissions of the same information once the computed certifier generated by calculating f_{KY}(ID, X, k) is equal (or IDENTICAL) to the received certifier S (if received communication number k is also not out-of-bounds) (Col. 13, lines 19-27). But this is the opposite behavior as required by the claim, which *terminates said flow* when the compared signatures *are not identical*. Thus, Akiyama does not teach *if said test signature and said validation signature are not identical, terminating said flow*.

For the reasons stated above, claim 1 patentably distinguishes over the cited prior art, and the rejection of claim 1 under 35 U.S.C. §103(a) should be withdrawn. Accordingly, claim 1 is in allowable condition.

Because claims 2-8 depend from and further limit claim 1, claims 2-8 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art. For example, claim 3 recites the method of claim 1 wherein said hashing comprises *computing a checksum* from said non-mutable field values. This feature is not taught or suggested by the cited prior art. The Office Action, on pages 4-5 cited Col. 13, lines 17-23 of Akiyama as teaching this feature. However, Applicants were unable to determine how or where the cited portion teaches *computing a checksum*. If the rejection of claim 3 is to be maintained, Applicants respectfully request that it be pointed out with

particularity where the cite prior art teaches such *computing a checksum* from said non-mutable field values.

As an additional example, claim 5 recites the method of claim 1 wherein said hashing comprises *computing a strong hash value* from said non-mutable field values. This feature is not taught or suggested by the cited prior art. The Office Action, on page 5 cited Col. 13, lines 48-59 of Akiyama as teaching this feature. However, Applicants were unable to determine how or where the cited portion teaches *computing a strong hash value*. If the rejection of claim 3 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cite prior art teaches such a *computing a strong hash value* from said non-mutable field values.

Claims 18-25

Claim 18 recites an apparatus for blocking attacks on a computer network. The apparatus includes a packet hashing device configured to receive original packets and corresponding retransmit packets from a network. Each said original packet and corresponding retransmit packet belong to a flow. Each said original packet and corresponding retransmit packet has a plurality of non-mutable field values. The packet hashing device employs a packet hashing algorithm to hash said non-mutable field values of each said original packet to produce a validation signature of each said original packet and to hash said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet. The apparatus also includes a flow cache connected to said packet hashing device and configured to store said validation signatures. The apparatus further includes a comparator operably connected to said flow cache configured to compare said validation signature to said test signature and having an output. The apparatus also includes a flow terminator receiving said output of said comparator and configured to terminate said flow if

said output indicates that said test signature and said validation signature are not identical.

The cited reference does not teach or suggest an apparatus which includes (a) a packet hashing device employing a packet hashing algorithm to *hash said non-mutable field values of each said original packet to produce a validation signature of each said original packet* and to *hash said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet*, (b) a comparator operably connected to said flow cache configured to *compare said validation signature to said test signature* and having an output, or (c) a flow terminator receiving said output of said comparator and *configured to terminate said flow if said output indicates that said test signature and said validation signature are not identical*. Rather, as argued above in connection with claim 1, Akiyama is directed to applying a certifying function f_{KY} using key KY and the received parameters ID, X, and k from the signal to verify the integrity and security of the signal. If the signal is verified, then operation X is carried out and receiving device 20 stores the received communication number k plus addition number Δk. Therefore, claim 18 is allowable for similar reasons as argued above in connection with claim 1.

Furthermore, the cited reference does not teach an apparatus having a *packet hashing device* employing a packet hashing algorithm to *hash said non-mutable field values of each said original packet to produce a validation signature* of each said original packet *and to hash said non-mutable field values of each said corresponding retransmit packet to produce a test signature* of each said corresponding retransmit packet. Rather, Akiyama discloses applying a unidirectional function f_{KY} at the transmission device 10, and later again applying the unidirectional function f_{KY} at the receiving device 20. However, Akiyama does not teach a *packet hashing device* employing a packet hashing algorithm to *hash said non-mutable field values of each said original packet to produce a validation*

signature of each said original packet *and to hash said non-mutable field values of each said corresponding retransmit packet to produce a test signature* of each said corresponding retransmit packet. This is because the unidirectional function f_{KY} is applied at two different locations in Akiyama, and not at a single *packet hashing device*. Akiyama does teach, in some instances, applying the unidirectional function f_{KY} on consecutively received signals, however, those generated values are never directly compared, as the result of the unidirectional function f_{KY} applied at the receiving device 20 is compared to the certifier S received from the transmission device 10, so the application of the unidirectional function f_{KY} on the consecutively received signals is not comparable to *producing a validation signature* and *a test signature*.

For the reasons stated above, claim 18 patentably distinguishes over the cited prior art, and the rejection of claim 18 under 35 U.S.C. §103(a) should be withdrawn. Accordingly, claim 18 is in allowable condition.

Because claims 19-25 depend from and further limit claim 18, claims 19-25 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Claims 10-17 and 26-49

Claims 10, 26, 34, and 42 recite limitation similar to those found in claim 1. Therefore, claims 10, 26, 34, and 42 are allowable for similar reasons as argued above in connection with claim 1.

For the reasons stated above, claims 10, 26, 34, and 42 patentably distinguishe over the cited prior art, and the rejection of claims 10, 26, 34, and 42 under 35 U.S.C. §103(a) should be withdrawn. Accordingly, claims 10, 26, 34, and 42 are in allowable condition.

Because claims 11-17, 27-33, 35-41, and 43-49 depend from and further limit claims 10, 26, 34, and 42, claims 11-17, 27-33, 35-41, and 43-49 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Newly Added Claims

Claims 50-51 have been added and are believed to be in allowable condition. Claim 50 depends from claim 1. Claim 51 depends from claim 18. Support for claims 50-51 is provided within the Specification, for example, in Fig. 2. No new matter has been added.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicant's Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Michael Ari Behar/

M. Ari Behar, Esq.
Attorney for Applicants
Registration No.: 58,203
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-129

Dated: December 26, 2007